

# Подход к идентификации инцидентов в компьютерной сети

Алексеев Д.И.

Харьковский национальный университет радиоэлектроники, [dimitry.alexeyev@gmail.com](mailto:dimitry.alexeyev@gmail.com)

*Need respond to an incidents that caused on the network at minimal time for realize the smooth functioning of a computer network. The control action is a response. This control action generated automatically. To resolve the incident use approach that provides choice from list of necessary actions.*

## ВВЕДЕНИЕ

Для обеспечения бесперебойного функционирования компьютерной сети организации необходимо своевременно реагировать на возникающие в сети инциденты. Решением проблемы является классификация инцидентов и сопоставление им управляющих действий. Целью исследования является разработка подхода по своевременной идентификации инцидентов в компьютерной сети.

## ИНЦИДЕНТЫ В КОМПЬЮТЕРНОЙ СЕТИ

Сбой в работе компьютерной сети является инцидентом. По происхождению инциденты могут быть различных видов:

1. Аппаратные инциденты  $H = \{h_i\}$ . Могут быть вызваны выходом из строя оборудования, отключением электропитания и т.п.
2. Программные инциденты  $P = \{p_j\}$ . Могут быть вызваны вследствие ошибок в программном обеспечении, перегрузки приложения поступающими данными и т.п.
3. Блокировка трафика  $T = \{t_k\}$ . Блокировка трафика может происходить вследствие перегрузки канала передачи данных.

В общем случае наличие в сети инцидента можно показать в следующем виде:

$$h_i \vee p_j \vee t_k \neq \emptyset \quad (1)$$

где  $h_i$  – аппаратный инцидент,  $p_j$  – программный инцидент,  $t_k$  – инцидент блокировки.

Для каждого инцидента или для группы инцидентов, входящих в определенное множество предусматривается наличие действия необходимого для устранения инцидента, действия также составляют множество, т.е.  $a_i \in A[1]$ .

К основным признакам наличия инцидентов в компьютерной сети можно отнести:

1. Появление записи об инциденте в журнале событий операционной системы или в журнале событий сетевых устройств.
2. Увеличение времени доступа к ресурсам компьютерной сети.
3. Увеличение времени задержек при передаче пакетов по каналам связи.

Для описанных признаков вводим множество наблюдаемых событий  $E = \{e_{pq}\}$ , где  $p$  – признак,  $q$  – текущий номер события.

Появление инцидента приводит к нарушению функционирования компьютерной сети. Своевременное обнаружение и устранение причин возникшего инцидента позволит минимизировать затраты, которые возникают по причине ненормального функционирования

компьютерной сети. Под нормальным функционированием компьютерной сети подразумевается соответствие состояния компьютерной сети заданным администратором сети параметрам  $F_i = F_0$  [2]. К таким параметрам относятся: бесперебойное функционирование аппаратной составляющей компьютерной сети (коммутаторов, маршрутизаторов, сетевых плат и т.п.); работа программных компонентов в соответствии с необходимыми для функционирования сети условиями – обеспечение необходимых значений параметров пропускной способности, соответствие заданным значениям параметров задержек и т.д.

### Идентификация инцидентов

Таким образом, одним из путей устранения возникающих в сети инцидентов может быть использование подхода, использующего для своей работы классификацию инцидентов, и который заключается в следующем.

1. Проводится анализ событий  $E$  для поиска признаков появления инцидента. По результатам анализа определяется наличие инцидентов, относящихся к одному из множеств: аппаратные к множеству  $H = \{h_0, h_1, \dots, h_n\}$ , т.е.  $h(e_i) \in H$ ; программные к множеству  $P = \{p_0, p_1, \dots, p_m\}$ , т.е.  $p(e_i) \in P$ ; инциденты блокировки трафика к множеству  $T = \{t_0, t_1, \dots, t_k\}$ , т.е.  $t(e_i) \in T$ .

2. Формируется сообщение администратору компьютерной сети.

3. Предпринимаются действия по устранению инцидента. Устранение производится путем запуска соответствующего управляющего воздействия  $a_i \in A$  из множества действий  $A = \{a_0, a_1, \dots, a_k\}$ .

### Выводы

Таким образом, существуют типизированные инциденты, для каждого из которых имеется определенное действие  $a_i$ , применение которого позволяет устранить данный инцидент, или

$$\forall I_i, \exists a_j, (S_i, a_j, S_j), I_j(S_j) = \emptyset \quad (2)$$

К действиям можно отнести: замену оборудования, восстановление электропитания, перезапуск системы, проведение обновления системы, перенаправление потока трафика, увеличение пропускной способности канала связи, внесение изменений в конфигурацию сетевого экрана и т.д. В результате своевременного применения действий влияние инцидентов на функционирование компьютерной сети будет минимизировано.

Для получения текущих значений параметров, которые необходимо контролировать в компьютерной сети рекомендуется использовать технологию «агент-менеджер». Использование подобной технологии позволит своевременно получать данные о состоянии контролируемых параметров, что позволит вовремя реагировать на их изменение. С использованием данного подхода появляется возможность накапливать статистическую информацию об изменении параметров и реализовать превентивные действия по предотвращению инцидентов [3].

Применение подхода к идентификации инцидентов, основанного на использовании классификации, позволяет сократить время на идентификацию инцидента, что в свою очередь положительно сказывается на времени, необходимом для устранения обнаруженных в компьютерной сети инцидентов.

## ЛИТЕРАТУРА

- [1] Хемди А. Таха Глава 17. Системы массового обслуживания // Введение в исследование операций = Operations Research: An Introduction — 7-е изд. — М.: «Вильямс», 2007. — С. 629-697. — ISBN 0-13-032374-8.
- Стюарт Рассел, Питер Норвиг. Искусственный интеллект: современный подход (AIMA): [пер. с англ.]. — 2-е изд. — М.: Вильямс, 2005. — 1424 p.
- Adnan Darwiche. Modeling and Reasoning with Bayesian Networks — Cambridge University Press, 2009. — 526 p. — ISBN 978-0521884389.